REMARKS:

In the outstanding Office Action, the Examiner noted that claims 1 and 3-12 were pending; rejected claims 1, 3-9, 11 and 12 under 35 U.S.C. § 102(e); and rejected claim 10 under 35 U.S.C. § 103(a). Claims 1, 3, 4 and 8-12 have been cancelled and claims 13-16 have been added. Thus, claims 5-7 and 13-16 are pending and under consideration. No new matter has been added. The rejections are traversed below.

REJECTION UNDER 35 U.S.C. § 102(e):

Claims 1, 3-9, 11 and 12 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Publication No. 2001/0044894 (Saito). Saito discusses shifting existing user authentication schemes based on a user ID and a password to a single authentication scheme using an integrated certificate (see, paragraphs 5 and 6). However, in Saito, either an integrated authentication server 2 or a DB server 5 confirms the integrated certificate and authentication server 2 acquires security information from server 3 (provided "for managing security information") to check the right of the user to access, e.g., DB server 5 (see, FIG. 1 and paragraph 35). When the right to access is authorized, authentication information such as a user ID and a password is sent to the DB server 5 which carries out the user's authentication process for the user by using the conventional user ID and password (see, paragraphs 35 and 36). Single sign-on is accomplished by subsequently transmitting the "already inputted integrated certificate" from the client 20 to application server 6 when access to application server 6 is desired by the client 20.

In contrast, the present invention enables a user of a variety of services to obtain a single common certificate information from a certificate authority and use the common certificate information as a certificate to receive any of the variety of services without requiring the user to notify the certificate authority of an ID and a password issued by a provider of a particular service (see, page 26, lines 4-14; FIGS. 6 and 8; and blocks S32-S33 in FIG.11 of the subject application).

For example, in the embodiment illustrated in FIG. 6 of the subject application, an available service management table establishes a link between a service ID of a common certificate information requesting party and the common certificate information. That is, service providing servers are not required to transmit a service specific user ID or password to a certificate authority, even when the certificate authority validates already issued common certificate information for use as a certificate for receiving any other service (see, blocks S17-S19 of FIG.9 and page 19, line 24 through page 20, line 14).

Independent claims 5-7 as amended recite that the present invention uses "common certificate information in common with a plurality of services" (e.g., claim 5, lines 3-4) "without requiring identification information and password information issued by the services" (e.g., claim 5, lines 6-7) to certify or authenticate a user to enable access to services.

As described in the embodiment illustrated in FIG. 11 of the subject application, when receiving an authentication request from a service providing server that has received a service access request from a user, a certificate authority determines whether the available service management table contains the requested service in association with the common certificate information specified in the request (see, blocks S32-S33 in FIG.11 and lines 4-14 on page 26). Accordingly, the present invention does not require the user ID or password that are specific to a service be exchanged between the service providing server and the certificate authority.

Saito does not teach or suggest a certificate authority certifying a user "without requiring identification and password information issued by the services". Instead, Saito is directed to using an integrated authentication server that recognizes user IDs and passwords associated with each requesting server, such as application servers and DB servers, and transmits access control information to each requesting server.

It is respectfully submitted that claim 5 and claims 6 and 7 which recite limitations similar to those discussed above from claim 5, are patentable over Saito.

REJECTION UNDER 35 U.S.C. § 103(a):

Claim 10 was rejected under 35 U.S.C. § 103(a) as unpatentable over Saito in view of U.S. Patent No. 6,128,740 (Curry). As mentioned above, dependent claim 10 has been cancelled and therefore, this rejection is moot.

NEW CLAIMS:

New claims 13-16 have been added to recite the features of the invention discussed above with varying scope. Proper support for new claims 13-16 can be found at least at FIGS. 6, 8, 9 and 11; page 17, line 8 through page 18, line; page 19, line 24; page 20, line 4; page 26, line 16; page 27, line 1; page 20, line 24 and page 21, line 14.

For at least the reasons discussed above, it is respectfully submitted that new claims 13-

16 patentably distinguish over the cited references.

CONCLUSION:

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 5/23/05

By: Richard A. Gollhofer
Richard A. Gollhofer
Registration No. 31,106

1201 New York Avenue, NW, Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

CERTIFICATE UNDER 37 CFR 1.8(a)
I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450
on 5/23/ ,20 05
STAAS & HALSEY
By: Richard A. Gollhofer
Date: 5/23/05